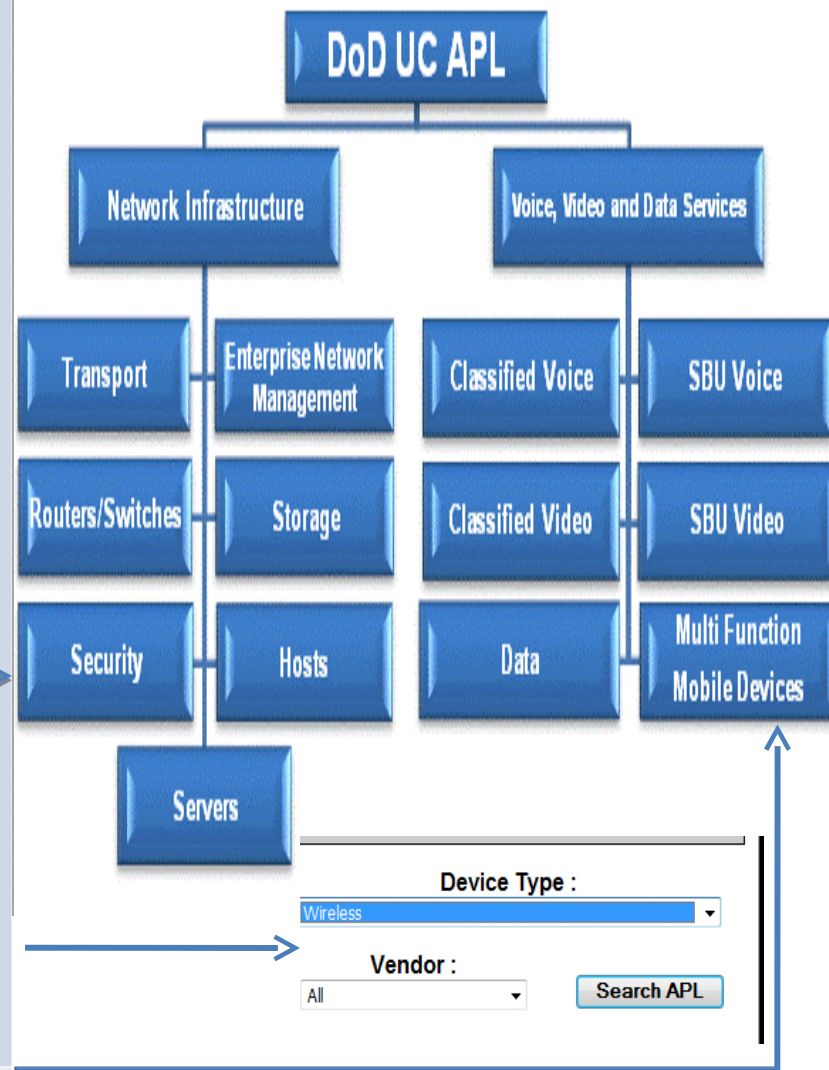


The Army Information Assurance-Approved Products List (AIA- APL) Categories can now found under the following Sections of the DoD UC APL **

| AIA-APL | DoD UC APL |
|---|--|
| Integrated Security Solution | Security |
| Network-Based Firewalls | |
| Network Based Intrusion Detection System/Intrusion Prevention Systems (IDS/IPS) | |
| Wireless Intrusion Detection System/Intrusion Prevention Systems (WIDS/WIPS) | |
| Enterprise Security Management/Management Consoles | |
| Security Information Management System (SIMS) | |
| Virutal Private Networks (VPNs) | |
| Network Access Control | |
| Routers with IA capabilities, firewalls, VPNs, IDS/IPS, NACs | |
| AVs, Wireless LAN Controllers, etc. | |
| Systems Integrity Solutions | |
| IA Tools for Wireless | |
| | Wireless (Located in the Device Type Drop Down Menu) |
| | Multi-Function Mobile Devices/Multimedia Mobile |



** Effective October 01, 2010 The Army implemented the DoD UC APL which is established in accordance with the UC Requirements (UCR 2008, Change 1) document. Its purpose is to maintain a single consolidated list of products that have completed Interoperability Certification (IA) certification. The DoD UC APL allows DoD Components to purchase and operate UC systems over all DoD network infrastructures. For questions regarding the UC APL please contact the UCCO at: UCCO@disa.mil For Cyber Tools Management questions please contact: armyiatools@us.army.mil

The Army Information Assurance-Approved Products List (AIA- APL) Other Specialty Tools

| Other Specialty Tools | Location |
|---|--|
| Wireless Network Discovery & Naval Research Labs (NRL), Flying Squirrel (free) | http://iase.disa.mil/tools/index.html |
| Secure Configuration Remediation Management System | |
| Network Assessment Tools Vulnerability Scanners | |
| PII Tool and Data Leakage/Loss Prevention Tools: Fidelis Security Systems Product Line: Software Version Release 5.0, 5.2, 5.3 Fidelis XPS CommandPost Appliance (Enterprise manager) Fidelis XPS Direct Models 100, 1000, & 2500 Fidelis XPS Scout (All-inOne) with CommandPost and Direct Sensors Netwitness Corporation Product Line: Software Version Release 8.0 and 9.0 Netwitness All in One/Integrated Solution Netwitness Decoder Appliance (Linux) Netwitness Informer Appliance version 2.0 (Windows 2003 Server) - PII Memo Netwitness Investigator Enterprise (Windows XP/Vista) | NOTE: Before deploying the PII Tools and Data Leakage/Loss Prevention please refer to MEMORANDUM 21 July 2009 Subject: Use of the Tools to Detect Potential Violations of Personally Identifiable Information (PII). available at: https://informationassurance.us.army.mil Select "Tools" CoN: Yes Date: 6/1/2010 |
| Data at Rest (DAR)- USB Memory Devices/Encrypted Removable Storage Media Mobile Armor, KeyArmor Metal Casing (4, 8, & 16 GB) Software Version: 3.0.1 Mobile Armor, KeyArmor Rugged Casing (2, 4, & 8 GB) Software Version: 3.0.1 Mobile Armor, KeyArmor Policy Server Software Version: 3.1 Key Armor Module 3.0 (Management Software for KeyArmor Approved Functions: Thumb Drive for Windows 2000, Windows 7, Windows XP, and Windows Vista | www.esi.mil NOTE: CYBERCOM is recommending using the ESI website where Mobile Armor is listed as an approved DAR product for DoD procurement |
| Government-off-the-shelf, Purge Effects | https://www.acert.1stiocmd.army.mil |
| Government-off-the-shelf, Universal Purge (UPT) | Request UPT Application by emailing: melvin.thomas3@us.army.mil |
| SNORT (Open Source Technology) (Software Only) | https://www.acert.1stiocmd.army.mil/tools/snort/ NOTE: AUTHORIZED for DOWNLOAD FROM THE ACERT website |
| CryptoMod Communications Security (COMSEC) Equipment | https://cryptomod.kc.us.army.mil NOTE: This website provides the Approved CryptoMod COMSEC equipment |
| A2TOC Directed Tools | NIPR Version (QTip, ACERT/RCERT) : https://www.rcert-c.army.mil/tools_index.htm SIPR Version: https://www.rcert-c.army.smil.mil |
| Malicious Code Detectors DISCLAIMER: Anti-Virus The DoD Antivirus Software License Agreement with Network Associates and Symantec allows active DoD employees to utilize the antivirus software for home use. Home use of the antivirus products will not only protect personal PCs at home, but will also potentially lessen the threat of employees bringing malicious logic into work and compromising DoD networks. Contractors are excluded from using the software at home or on any other systems not belonging to the DoD. Contractors may only use the software on systems of which are the property of the DoD | McAfee & Symantec https://www.acert.1stiocmd.army.mil/Antivirus/ Please note that the only approved AV software are the free tools on the ACERT web site. |
| KVM Switches | For guidance on approved KVM Switches Please read the DISA STIG Titled |